

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-326695
 (43)Date of publication of application : 22.11.2001

(51)Int.CI.

H04L 12/66
 G06F 13/00
 H04L 12/28
 H04L 12/56

(21)Application number : 2000-146256

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 18.05.2000

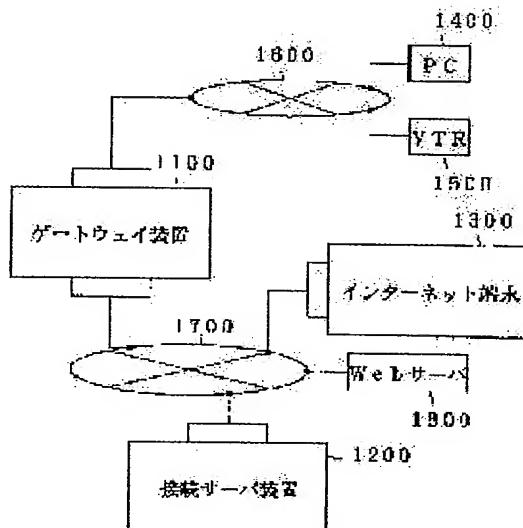
(72)Inventor : TAKEDA HIDETOSHI

(54) GATEWAY UNIT, CONNECTION SERVER UNIT, INTERNET TERMINAL, NETWORK SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a gateway unit that interconnects a private network and the Internet, and relieves the load of complicated processings for maintaining security.

SOLUTION: An Internet terminal 1300, connected to the Internet 1700, communicates with a PC 1400 or a VTR 1500 as a private terminal. A connection server unit 1200 connected to the Internet authenticates the communication to the private network 1600. The gateway unit 1100 receives only an encrypted packet, received from the connection server unit 1200, to maintain security of the private network 1600 and to reduce the processing load of the gateway unit 1100 to a low level.



LEGAL STATUS

[Date of request for examination] 16.04.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-326695

(P2001-326695A)

(43)公開日 平成13年11月22日 (2001.11.22)

(51)Int.Cl.

H 04 L 12/66
G 06 F 13/00
H 04 L 12/28
12/56

識別記号

3 5 1

F I

G 06 F 13/00
H 04 L 11/20
11/00
11/20

マーコード(参考)

3 5 1 Z 5 B 0 8 9
B 5 K 0 3 0
3 1 0 D 5 K 0 3 3
1 0 2 A

審査請求 未請求 請求項の数26 O L (全 20 頁)

(21)出願番号

特願2000-146256(P2000-146256)

(22)出願日

平成12年5月18日 (2000.5.18)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 武田 英俊

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 100084364

弁理士 岡本 宜喜

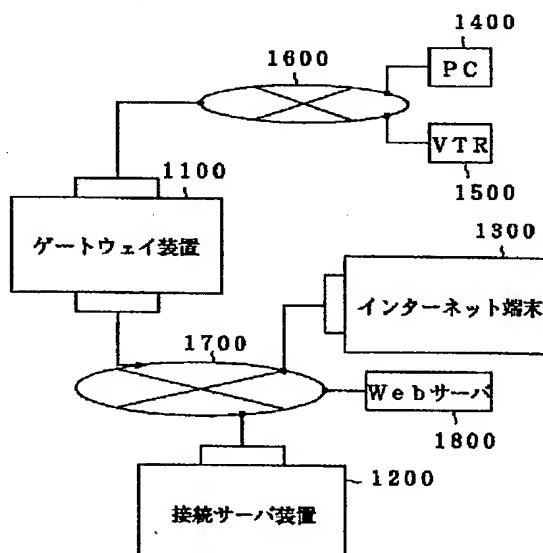
F ターム(参考) 5B089 GA31 HA10 KA17 KB06 KB13
KC52 KC58 KH30
5K030 GA15 HD03 HD06 HD09 JA05
JT02
5K033 AA08 CB02 CB09 CC01 DA06
DB18

(54)【発明の名称】 ゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステム

(57)【要約】

【課題】 プライベート・ネットワークとインターネットを相互に接続するゲートウェイ装置において、セキュリティを維持するための複雑な処理を軽減すること。

【解決手段】 インターネット1700に接続されたインターネット端末1300から、プライベート端末装置としてPC1400又はVTR1500と通信する。このときプライベート・ネットワーク1600への通信を行うための認証を、インターネットに接続された接続サーバ装置1200で行う。ゲートウェイ装置1100は接続サーバ装置1200から受け取る暗号化されたパケットのみを受信することで、プライベート・ネットワーク1600のセキュリティを保ち、且つゲートウェイ装置1000の処理負担を小さくすることができる。



【特許請求の範囲】

【請求項1】 プライベート端末装置が接続されたプライベート・ネットワークとインターネットとを接続するゲートウェイ装置であって、
前記プライベート・ネットワークからパケットを受信する第1のパケット受信手段と、
前記プライベート・ネットワークに対してパケットを送信する第1のパケット送信手段と、
前記インターネットからパケットを受信する第2のパケット受信手段と、
前記インターネットに対してパケットを送信する第2のパケット送信手段と、
前記第2のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、
前記第1のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行って前記第2のパケット送信手段に与えると共に、前記第2のパケット受信手段又は前記暗号解読手段から入力されたパケットのアドレス及びプロトコルの変換を行って前記第1のパケット送信手段に与えるパケット変換手段と、を具備し、
前記第2のパケット受信手段は、
暗号化されたパケットを受信した場合に暗号化パケットを前記暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットを前記パケット変換手段に与え、
前記暗号解読手段は、
暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするゲートウェイ装置。

【請求項2】 前記パケット変換手段は、
代理サーバ機能を持ち、前記プライベート・ネットワークから受け取ったパケットの発信元IPアドレスとして前記インターネットで使用する単一のIPアドレスを附加して出力することを特徴とする請求項1記載のゲートウェイ装置。

【請求項3】 前記暗号解読手段は、
前記インターネットに接続され、予め決められた接続サーバ装置のIPアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とする請求項1記載のゲートウェイ装置。

【請求項4】 前記パケット変換手段は、
前記パケット変換手段によって変換し、前記プライベート端末装置に対して送信したパケットに対する応答として前記プライベート端末装置から出力された応答パケット、及び前記暗号解読手段から出力されたパケットのみを受け取ることを特徴とする請求項3記載のゲートウェイ装置。

【請求項5】 前記パケット変換手段は、
前記暗号解読手段から受け取ったパケットのデータ部分

を送信パケットとして前記第1のパケット送信手段に与えることを特徴とする請求項1～4のいずれか1項記載のゲートウェイ装置。

【請求項6】 前記パケット変換手段は、
前記第2のパケット受信手段を介して前記接続サーバ装置の問い合わせパケットを受け取った場合、前記接続サーバ装置のIPアドレスを含む応答パケットを前記第2のパケット送信手段に出力することを特徴とする請求項3～5のいずれか1項記載のゲートウェイ装置。

【請求項7】 前記パケット変換手段は、
Webサーバ機能を持ち、前記暗号化手段から受け取ったパケットを前記Webサーバによって処理し、処理の結果によって生成したパケットを前記第1のパケット送信手段に与えることを特徴とする請求項1～6のいずれか1項記載のゲートウェイ装置。

【請求項8】 プライベート端末装置が接続されたプライベート・ネットワークとインターネットとを接続するゲートウェイ装置であって、

前記プライベート・ネットワークからパケットを受信する第1のパケット受信手段と、
前記プライベート・ネットワークに対してパケットを送信する第1のパケット送信手段と、
前記インターネットからパケットを受信する第2のパケット受信手段と、
前記インターネットに対してパケットを送信する第2のパケット送信手段と、

前記第2のパケット受信手段で受信したパケットの少なくともデータ部分を暗号化した暗号化パケットを前記第2のパケット送信手段に与える暗号化手段と、

前記第2のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、
前記第1のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行ったパケットを前記暗号化手段に出力すると共に、前記暗号解読手段から受け取ったパケットのアドレス及びプロトコルの変換を行って前記第1のパケット送信手段に与えるパケット変換手段と、を具備し、
前記第2のパケット受信手段は、

受信したパケットを前記暗号解読手段に与え、
前記暗号解読手段は、
暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするゲートウェイ装置。

【請求項9】 前記パケット変換手段は、
前記第1のパケット受信手段から受け取ったパケットを、前記インターネットに接続されて予め決められた接続サーバ装置宛のパケットとして、前記暗号化手段に与えることを特徴とする請求項8記載のゲートウェイ装置。

【請求項10】 前記暗号解読手段は、
前記インターネットに接続され、予め決められた接続サーバ装置のIPアドレスを送信元としたパケットを入力

し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とする請求項8記載のゲートウェイ装置。

【請求項11】 前記パケット変換手段は、前記第1のパケット受信手段から受け取ったパケットを、前記インターネットに接続されて予め決められた接続サーバ装置宛のパケットとして前記暗号化手段に出力し、

前記暗号解読手段は、前記接続サーバ装置のIPアドレスを送信元としたパケットを対象とし、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とする請求項8記載のゲートウェイ装置。

【請求項12】 前記パケット変換手段は、前記暗号解読手段から受け取ったパケットのデータ部分を送信パケットとして前記第1のパケット送信手段に与えると共に、前記第1のパケット受信手段から受け取ったパケットをデータ部分に含み、前記接続サーバ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とする請求項1記載のゲートウェイ装置。

【請求項13】 前記パケット変換手段は、前記第2のパケット受信手段を介して前記接続サーバ装置の問い合わせパケットを受け取った場合、前記接続サーバ装置のIPアドレスを含む応答パケットを前記第2のパケット送信手段に与えることを特徴とする請求項9～12のいずれか1項記載のゲートウェイ装置。

【請求項14】 プライベート・ネットワークに接続されたゲートウェイ装置とインターネットを介して通信を行う接続サーバ装置であって、

前記インターネットからパケットを受信するパケット受信手段と、前記インターネットに対してパケットを送信するパケット送信手段と、

前記パケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記パケット送信手段に与える認証手段と、

パケットのデータ部分を暗号化して前記パケット送信手段に与える暗号化手段と、

前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行った変換パケットを前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与えるパケット変換手段と、を具備することを特徴とする接続サーバ装置。

【請求項15】 前記パケット変換手段は、前記パケット受信手段から受け取ったパケットをデータ部分に含み、前記ゲートウェイ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とする請求項1

4記載の接続サーバ装置。

【請求項16】 前記認証手段は、認証結果として認証IDを出力し、

前記パケット変換手段は、前記認証手段が出力する前記認証ID、及び前記パケット受信手段から受け取るパケットに含まれる認証IDを比較することによって、前記インターネット端末が認証されているか否かを判断し、認証結果が一致する場合にパケット変換することを特徴とする請求項14又は15記載の接続サーバ装置。

【請求項17】 プライベート・ネットワークに接続されたゲートウェイ装置とインターネットを介して通信を行う接続サーバ装置であって、

前記インターネットからパケットを受信するパケット受信手段と、

前記インターネットに対してパケットを送信するパケット送信手段と、

前記パケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記パケット送信手段に与える認証手段と、

パケットのデータ部分を暗号化して前記パケット送信手段に与える暗号化手段と、

前記パケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、

前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末機器への転送を求めるパケットを前記パケット受信手段を介して受け取り、アドレス及びプロトコルの変換を行った変換パケットを前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与えるパケット変換手段と、を具備し、

前記パケット受信手段は、データ部分の暗号化されたパケットを受信した場合には暗号化パケットを前記暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットを前記パケット変換手段に与え、

前記暗号解読手段は、暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とする接続サーバ装置。

【請求項18】 前記暗号解読手段は、前記ゲートウェイ装置のIPアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とする請求項17記載の接続サーバ装置。

【請求項19】 前記パケット変換手段は、前記暗号解読手段から受け取ったパケットのデータ部分に含まれるパケットを送信パケットとして前記パケット送信手段に与えると共に、前記パケット受信手段から受け取ったパケットをデータ部分に含み、前記ゲートウェイ

イ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とする請求項17記載の接続サーバ装置。

【請求項20】 前記パケット変換手段は、代理サーバ機能を持ち、前記暗号解読手段から受け取ったパケットのデータ部分に含まれるパケットの発信元IPアドレスとして、前記接続サーバ装置のIPアドレスを付加して出力することを特徴とする請求項19記載の接続サーバ装置。

【請求項21】 前記認証手段は、

認証結果として認証IDを出し、前記パケット変換手段は、

前記認証手段が outputする前記認証ID、及び前記パケット受信手段から受け取るパケットに含まれる認証IDを比較することによって、前記インターネット端末が認証されているか否かを判断し、認証結果が一致する場合にパケット変換することを特徴とする請求項17～20のいずれか1項記載の接続サーバ装置。

【請求項22】 前記パケット変換手段は、

Webサーバ機能を持ち、前記暗号化手段から受け取ったパケットを前記Webサーバによって処理し、処理の結果によって生成したパケットを前記第1のパケット送信手段に与えることを特徴とする請求項17～21のいずれか1項記載の接続サーバ装置。

【請求項23】 インターネットに接続され、プライベート・ネットワークに接続されたプライベート端末機器との間で通信を行うインターネット端末であって、前記インターネットからパケットを受信するパケット受信手段と、

前記インターネットに対してパケットを送信するパケット送信手段と、

前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、

前記接続サーバ装置から前記パケット受信手段を介して認証結果を受け取り、前記接続サーバ装置に対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記パケット送信手段に与えるパケット生成手段と、を具備することを特徴とするインターネット端末。

【請求項24】 前記認証要求手段は、

前記接続サーバ装置から認証結果として認証IDを受け取り、前記認証IDを前記パケット生成手段に与えることを特徴とする請求項23記載のインターネット端末。

【請求項25】 プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するネットワークシステムであって、

前記ゲートウェイ装置は、前記プライベートネットワークと前記インターネットの両者に接続され、

前記プライベート・ネットワークからパケットを受信する第1のパケット受信手段と、

前記プライベート・ネットワークに対してパケットを送信する第1のパケット送信手段と、

前記インターネットからパケットを受信する第2のパケット受信手段と、

前記インターネットに対してパケットを送信する第2のパケット送信手段と、

前記第2のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、

前記第1のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを前記第2のパケット送信手段に与えると共に、前記第2のパケット受信手段から出力されたパケット又は前記暗号解読手段から出力された暗号解読済のパケットに対して、アドレス及びプロトコルの変換を行ったパケットを前記第1のパケット送信手段に与える第1のパケット変換手段と、を具備するものであり、

前記接続サーバ装置は、

前記インターネットに接続され、

前記インターネットからパケットを受信する第3のパケット受信手段と、

前記インターネットに対してパケットを送信する第3のパケット送信手段と、

前記第3のパケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記第3のパケット送信手段に与える認証手段と、パケットのデータ部分を暗号化した暗号化パケットを前記パケット送信手段に与える暗号化手段と、

前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行って前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与える第2のパケット変換手段と、を具備するものであり、前記インターネット端末は、

前記インターネットからパケット受信する第4のパケット受信手段と、

前記インターネットに対してパケットを送信する第4のパケット送信手段と、

前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、

前記接続サーバ装置から前記第4のパケット受信手段を介して認証結果を受け取り、前記接続サーバに対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記第4のパケット送信手段に与えるパケット生成手段と、を具備するものであることを特徴とするネットワークシステム。

【請求項26】 プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するネットワークシステムであって、

前記ゲートウェイ装置は、

前記プライベートネットワークと前記インターネットの両者に接続され、

前記プライベート・ネットワークからパケットを受信する第1のパケット受信手段と、

前記プライベート・ネットワークに対してパケットを送信する第1のパケット送信手段と、

前記インターネットからパケットを受信する第2のパケット受信手段と、

前記インターネットに対してパケットを送信する第2のパケット送信手段と、

パケットのデータ部分を暗号化した暗号化パケットを前記第2のパケット送信手段に与える第1の暗号化手段と、

前記第2のパケット受信手段で受信したパケットの少なくともデータ部分を解読する第1の暗号解読手段と、

前記第1のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを前記第1の暗号化手段

に与えると共に、前記第1の暗号解読手段から出力された暗号解読済のパケットに対して、アドレス及びプロトコルの変換を行ったパケットを前記第1のパケット送信手段に与える第1のパケット変換手段と、を具備するものであり、

前記接続サーバ装置は、

前記インターネットに接続され、

前記インターネットからパケットを受信する第3のパケット受信手段と、

前記インターネットに対してパケットを送信する第3のパケット送信手段と、

前記第3のパケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記第3のパケット送信手段に与える認証手段と、パケットのデータ部分を暗号化した暗号化パケットを前記第3のパケット送信手段に与える暗号化手段と、

前記第3のパケット受信手段で受信したパケットの少なくともデータ部分を解読する第2の暗号解読手段と、

前記認証手段によって認証された前記インターネット端

末から、前記プライベート・ネットワークに接続されたプライベート端末機器への転送を求めるパケットを前記第3のパケット受信手段を介して受け取り、アドレス及びプロトコルの変換を行ったものを変換パケットとして前記ゲートウェイ装置宛のパケットとして出力する際に、データ部分の暗号化されたパケットを受信した場合には暗号化パケットを前記第2の暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットをそのまま変換パケットに変換する共に、前記第2の暗号解読手段から出力されたパケットを変換パケットに変換する第2のパケット変換手段と、を具備するものであり、

前記インターネット端末は、

前記インターネットからパケット受信する第4のパケット受信手段と、

前記インターネットに対してパケットを送信する第4のパケット送信手段と、

前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、

前記接続サーバ装置から前記第4のパケット受信手段を介して認証結果を受け取り、前記接続サーバに対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記第4のパケット送信手段に与えるパケット生成手段と、を具備するものであることを特徴とするネットワークシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、プライベート・ネットワークとインターネットとを相互に接続するための技術に係わり、特にゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステムに関する。

【0002】

【従来の技術】 これまで、プライベート・ネットワーク（インターネット）とインターネットを接続する場合、両方のネットワークが接続される位置にゲートウェイ装置を設置し、パケットを相互に転送することで2つのネットワークを相互接続していた。このようなゲートウェイ装置はルータとも呼ばれることがある。しかしながら、パケットを相互に転送するだけのゲートウェイ装置では、インターネットから、プライベート・ネットワークに接続されたプライベート端末装置に対して自由にアクセスができるため、不特定のユーザから不正なアクセスを受けてしまう危険性があった。

【0003】 このような不正なアクセスを防止し、プライベート・ネットワークのセキュリティを確保するためには、プライベート・ネットワークとインターネットと

の間にゲートウェイ装置を接続する場合、パケットそのまま転送せず、ファイア・ウォールと呼ばれる機能を設けることが多い。このようなファイア・ウォールでは、インターネットからプライベート・ネットワークに接続されたプライベート端末装置に対してパケットを直接に転送しないようにすることで、プライベート・ネットワークのセキュリティを確保することができる。

【0004】一方、ゲートウェイ装置では、代理サーバ（プロキシ・サーバ）機能を持つことによって、プライベート・ネットワークに接続されたプライベート端末装置から、インターネットに接続されたWebサーバ等へのアクセスを可能にすることができる。このような代理サーバは、プライベート・ネットワークに接続されたプライベート端末装置に対してWebサーバとして動作し、プライベート端末装置から受け取った要求を自らの要求としてインターネットに送信する。そしてこの要求の結果、インターネットを介して受け取った応答を、プライベート・ネットワーク内の要求を行ったプライベート端末装置に転送する。

【0005】プライベート・ネットワークとインターネットの両方に接続された代理サーバがこのような動作を行うことで、プライベート・ネットワークとインターネットとの間で直接パケットの転送を行わなくとも、プライベート・ネットワークからインターネットのWebサーバへのアクセスが実現できる。なお、この代理サーバの機能はIETF（The Internet Engineering Task Force）のRFC（Request for Comments）2616 Hypertext Transfer Protocol 1.1で定められている。

【0006】またこのようなファイア・ウォールでは、インターネットからプライベート・ネットワークへのアクセスを行う場合、ゲートウェイ装置においてインターネットに接続された端末やユーザの認証を行い、認証の結果許可された端末及びユーザが発信したパケットのみを転送するようにしている。このようなパケットの転送機能によって、不特定のユーザからの不正なアクセスを防ぐことができる。

【0007】一方、複数のプライベート・ネットワーク同士を、インターネットを介して相互に接続する仮想プライベート・ネットワーク（VPN: Virtual Private Network）が知られている。この仮想プライベート・ネットワークでは、プライベート・ネットワークとインターネットを接続するゲートウェイ装置において、プライベート・ネットワーク内のパケットを、インターネットを介して別のゲートウェイ装置に転送する。これを受けた別のゲートウェイ装置は、受信したパケットをプライベート・ネットワークに送信する。

【0008】例えば2つのプライベート・ネットワーク、即ちネットワーク1とネットワーク2があり、それぞれゲートウェイ1とゲートウェイ2を介してインターネットに接続されていたとする。ネットワーク1に接続

された端末からネットワーク2に接続されたサーバにパケットを送信する場合、このパケットはまずゲートウェイ1に送られる。ゲートウェイ1は、パケットの宛先アドレスからサーバがネットワーク2に接続された装置であると判断し、受信したパケットを、インターネットを介してゲートウェイ2に向けて送信する。一方これを受信したゲートウェイ2は、受信したパケットをサーバに對して送信する。

【0009】このように仮想プライベート・ネットワークでは、複数のゲートウェイ装置がインターネットを介してパケットの転送を行うことで、複数のプライベート・ネットワーク同士が相互に接続されているのと同等の効果を得ることができる。なお、仮想プライベート・ネットワークの詳細に関しては、例えばIETFのRFC2764A Framework for IP Based Virtual Private Networkに記載されている。

【0010】

【発明が解決しようとする課題】従来、セキュリティを確保した上でプライベート・ネットワークとインターネットを接続する場合、上述のような代理サーバ機能によってプライベート・ネットワークからインターネットへの通信を可能にする一方で、インターネットからプライベート・ネットワークへのパケットの転送を制限したり、また事前に認証を行うといった方法を用いていた。

【0011】しかしながら、高いセキュリティを保った上でインターネットからプライベート・ネットワークへのアクセスを可能にするためには、ゲートウェイ装置において複雑な認証手順を設定したり、またインターネットから要求を受け付けるためのサーバ機能が必要となる。このような機能を実現することは、例えば家庭内などの小規模なプライベート・ネットワークをインターネットに接続するゲートウェイ装置では、大きな負担となってしまうという課題があった。

【0012】本発明は、このような従来の問題点に鑑みてなされたものであって、ゲートウェイ装置の負担を軽減しつつ、プライベート・ネットワークのセキュリティを確保し、かつインターネットからプライベート・ネットワークに接続されたプライベート端末装置へのアクセスを可能にするゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステムを夫々実現することを目的とする。

【0013】

【課題を解決するための手段】本願の請求項1の発明は、プライベート端末装置が接続されたプライベート・ネットワークとインターネットとを接続するゲートウェイ装置であって、前記プライベート・ネットワークからパケットを受信する第1のパケット受信手段と、前記プライベート・ネットワークに対してパケットを送信する第1のパケット送信手段と、前記インターネットからパケットを受信する第2のパケット受信手段と、前記イン

ターネットに対してパケットを送信する第2のパケット送信手段と、前記第2のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、前記第1のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行って前記第2のパケット送信手段に与えると共に、前記第2のパケット受信手段又は前記暗号解読手段から入力されたパケットのアドレス及びプロトコルの変換を行って前記第1のパケット送信手段に与えるパケット変換手段と、を具備し、前記第2のパケット受信手段は、暗号化されたパケットを受信した場合に暗号化パケットを前記暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットを前記パケット変換手段に与え、前記暗号解読手段は、暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするものである。

【0014】本願の請求項2の発明は、請求項1のゲートウェイ装置において、前記パケット変換手段は、代理サーバ機能を持ち、前記プライベート・ネットワークから受け取ったパケットの発信元IPアドレスとして前記インターネットで使用する単一のIPアドレスを付加して出力することを特徴とするものである。

【0015】本願の請求項3の発明は、請求項1のゲートウェイ装置において、前記暗号解読手段は、前記インターネットに接続され、予め決められた接続サーバ装置のIPアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とするものである。

【0016】本願の請求項4の発明は、請求項3のゲートウェイ装置において、前記パケット変換手段は、前記パケット変換手段によって変換し、前記プライベート端末装置に対して送信したパケットに対する応答として前記プライベート端末装置から出力された応答パケット、及び前記暗号解読手段から出力されたパケットのみを受け取ることを特徴とするものである。

【0017】本願の請求項5の発明は、請求項1～4のいずれか1項のゲートウェイ装置において、前記パケット変換手段は、前記暗号解読手段から受け取ったパケットのデータ部分を送信パケットとして前記第1のパケット送信手段に与えることを特徴とするものである。

【0018】本願の請求項6の発明は、請求項3～5のいずれか1項のゲートウェイ装置において、前記パケット変換手段は、前記第2のパケット受信手段を介して前記接続サーバ装置の問い合わせパケットを受け取った場合、前記接続サーバ装置のIPアドレスを含む応答パケットを前記第2のパケット送信手段に出力することを特徴とするものである。

【0019】本願の請求項7の発明は、請求項1～6のいずれか1項のゲートウェイ装置において、前記パケット変換手段は、Webサーバ機能を持ち、前記暗号化手

段から受け取ったパケットを前記Webサーバによって処理し、処理の結果によって生成したパケットを前記第1のパケット送信手段に与えることを特徴とするものである。

【0020】本願の請求項8の発明は、プライベート端末装置が接続されたプライベート・ネットワークとインターネットとを接続するゲートウェイ装置であって、前記プライベート・ネットワークからパケットを受信する第1のパケット受信手段と、前記プライベート・ネットワークに対してパケットを送信する第1のパケット送信手段と、前記インターネットからパケットを受信する第2のパケット受信手段と、前記インターネットに対してパケットを送信する第2のパケット送信手段と、パケットのデータ部分を暗号化した暗号化パケットを前記第2のパケット送信手段に与える暗号化手段と、前記第2のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、前記第1のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行ったパケットを前記暗号化手段に出力すると共に、前記暗号解読手段から受け取ったパケットのアドレス及びプロトコルの変換を行って前記第1のパケット送信手段に与えるパケット変換手段と、を具備し、前記第2のパケット受信手段は、受信したパケットを前記暗号解読手段に与え、前記暗号解読手段は、暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするものである。

【0021】本願の請求項9の発明は、請求項8のゲートウェイ装置において、前記パケット変換手段は、前記第1のパケット受信手段から受け取ったパケットを、前記インターネットに接続されて予め決められた接続サーバ装置宛のパケットとして、前記暗号化手段に与えることを特徴とするものである。

【0022】本願の請求項10の発明は、請求項8のゲートウェイ装置において、前記暗号解読手段は、前記インターネットに接続され、予め決められた接続サーバ装置のIPアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とするものである。

【0023】本願の請求項11の発明は、請求項8のゲートウェイ装置において、前記パケット変換手段は、前記第1のパケット受信手段から受け取ったパケットを、前記インターネットに接続されて予め決められた接続サーバ装置宛のパケットとして前記暗号化手段に出力し、前記暗号解読手段は、前記接続サーバ装置のIPアドレスを送信元としたパケットを対象とし、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とするものである。

【0024】本願の請求項12の発明は、請求項11のゲートウェイ装置において、前記パケット変換手段は、

前記暗号解読手段から受け取ったパケットのデータ部分を送信パケットとして前記第1のパケット送信手段に与えると共に、前記第1のパケット受信手段から受け取ったパケットをデータ部分に含み、前記接続サーバ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とするものである。

【0025】本願の請求項13の発明は、請求項9～12のいずれか1項のゲートウェイ装置において、前記パケット変換手段は、前記第2のパケット受信手段を介して前記接続サーバ装置の問い合わせパケットを受け取った場合、前記接続サーバ装置のIPアドレスを含む応答パケットを前記第2のパケット送信手段に与えることを特徴とするものである。

【0026】本願の請求項14の発明は、プライベート・ネットワークに接続されたゲートウェイ装置とインターネットを介して通信を行う接続サーバ装置であって、前記インターネットからパケットを受信するパケット受信手段と、前記インターネットに対してパケットを送信するパケット送信手段と、前記パケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記パケット送信手段に与える認証手段と、パケットのデータ部分を暗号化して前記パケット送信手段に与える暗号化手段と、前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行った変換パケットを前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与えるパケット変換手段と、を具備することを特徴とするものである。

【0027】本願の請求項15の発明は、請求項14の接続サーバ装置において、前記パケット変換手段は、前記パケット受信手段から受け取ったパケットをデータ部分に含み、前記ゲートウェイ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とするものである。

【0028】本願の請求項16の発明は、請求項14又は15の接続サーバ装置において、前記認証手段は、認証結果として認証IDを出力し、前記パケット変換手段は、前記認証手段が outputする前記認証ID、及び前記パケット受信手段から受け取るパケットに含まれる認証IDを比較することによって、前記インターネット端末が認証されているか否かを判断し、認証結果が一致する場合にパケット変換することを特徴とするものである。

【0029】本願の請求項17の発明は、プライベート・ネットワークに接続されたゲートウェイ装置とインターネットを介して通信を行う接続サーバ装置であって、前記インターネットからパケットを受信するパケット受信手段と、前記インターネットに対してパケットを送信

するパケット送信手段と、前記パケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記パケット送信手段に与える認証手段と、パケットのデータ部分を暗号化して前記パケット送信手段に与える暗号化手段と、前記パケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末機器への転送を求めるパケットを前記パケット受信手段を介して受け取り、アドレス及びプロトコルの変換を行った変換パケットを前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与えるパケット変換手段と、を具備し、前記パケット受信手段は、データ部分の暗号化されたパケットを受信した場合には暗号化パケットを前記暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットを前記パケット変換手段に与え、前記暗号解読手段は、暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするものである。

【0030】本願の請求項18の発明は、請求項17の接続サーバ装置において、前記暗号解読手段は、前記ゲートウェイ装置のIPアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とするものである。

【0031】本願の請求項19の発明は、請求項17の接続サーバ装置において、前記パケット変換手段は、前記暗号解読手段から受け取ったパケットのデータ部分に含まれるパケットを送信パケットとして前記パケット送信手段に与えると共に、前記パケット受信手段から受け取ったパケットをデータ部分に含み、前記ゲートウェイ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とするものである。

【0032】本願の請求項20の発明は、請求項19の接続サーバ装置において、前記パケット変換手段は、代理サーバ機能を持ち、前記暗号解読手段から受け取ったパケットのデータ部分に含まれるパケットの発信元IPアドレスとして、前記接続サーバ装置のIPアドレスを付加して出力することを特徴とするものである。

【0033】本願の請求項21の発明は、請求項17～20のいずれか1項の接続サーバ装置において、前記認証手段は、認証結果として認証IDを出力し、前記パケット変換手段は、前記認証手段が outputする前記認証ID、及び前記パケット受信手段から受け取るパケットに含まれる認証IDを比較することによって、前記インターネット端末が認証されているか否かを判断し、認証結果が一致する場合にパケット変換することを特徴とするものである。

【0034】本願の請求項22の発明は、請求項17～

21のいずれか1項の接続サーバ装置において、前記パケット変換手段は、Webサーバ機能を持ち、前記暗号化手段から受け取ったパケットを前記Webサーバによって処理し、処理の結果によって生成したパケットを前記第1のパケット送信手段に与えることを特徴とするものである。

【0035】本願の請求項23の発明は、インターネットに接続され、プライベート・ネットワークに接続されたプライベート端末機器との間で通信を行うインターネット端末であって、前記インターネットからパケットを受信するパケット受信手段と、前記インターネットに対してパケットを送信するパケット送信手段と、前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、前記接続サーバ装置から前記パケット受信手段を介して認証結果を受け取り、前記接続サーバ装置に対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記パケット送信手段に与えるパケット生成手段と、を具備することを特徴とするものである。

【0036】本願の請求項24の発明は、請求項23のインターネット端末において、前記認証要求手段は、前記接続サーバ装置から認証結果として認証IDを受け取り、前記認証IDを前記パケット生成手段に与えることを特徴とするものである。

【0037】本願の請求項25の発明は、プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するネットワークシステムであって、前記ゲートウェイ装置は、前記プライベートネットワークと前記インターネットの両者に接続され、前記プライベート・ネットワークからパケットを受信する第1のパケット受信手段と、前記プライベート・ネットワークに対してパケットを送信する第1のパケット送信手段と、前記インターネットからパケットを受信する第2のパケット受信手段と、前記インターネットに対してパケットを送信する第2のパケット送信手段と、前記第2のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、前記第1のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを前記第2のパケット送信手段に与えると共に、前記第2のパケット受信手段から出力されたパケット又は前記暗号解読手段から出力された暗号解読済のパケットに対して、アドレス及びプロトコルの変換を行ったパケットを前記第1のパケット送信手段に与える第1のパケット変換手段と、を具備するものであり、前記接続サーバ装置は、前記インターネットに接続され、前記インターネットか

らパケットを受信する第3のパケット受信手段と、前記インターネットに対してパケットを送信する第3のパケット送信手段と、前記第3のパケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記第3のパケット送信手段に与える認証手段と、パケットのデータ部分を暗号化した暗号化パケットを前記パケット送信手段に与える暗号化手段と、前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行って前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与える第2のパケット変換手段と、を具備するものであり、前記インターネット端末は、前記インターネットからパケット受信する第4のパケット受信手段と、前記インターネットに対してパケットを送信する第4のパケット送信手段と、前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、前記接続サーバ装置から前記第4のパケット受信手段を介して認証結果を受け取り、前記接続サーバ装置に対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記第4のパケット送信手段に与えるパケット生成手段と、を具備することを特徴とするものである。

【0038】本願の請求項26の発明は、プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するネットワークシステムであって、前記ゲートウェイ装置は、前記プライベートネットワークと前記インターネットの両者に接続され、前記プライベート・ネットワークからパケットを受信する第1のパケット受信手段と、前記プライベート・ネットワークに対してパケットを送信する第1のパケット送信手段と、前記インターネットからパケットを受信する第2のパケット受信手段と、前記インターネットに対してパケットを送信する第2のパケット送信手段と、パケットのデータ部分を暗号化した暗号化パケットを前記第2のパケット送信手段に与える第1の暗号化手段と、前記第2のパケット受信手段で受信したパケットの少なくともデータ部分を解読する第1の暗号解読手段と、前記第1のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを前記第1の暗号化手段に与えると共に、前記第1の暗号解読手段から出力された暗号解読済のパケットに対して、アドレス及びプロトコルの変換を行ったパケットを前記第1のパケット送信手段に与える第1のパケット

変換手段と、を具備するものであり、前記接続サーバ装置は、前記インターネットに接続され、前記インターネットからパケットを受信する第3のパケット受信手段と、前記インターネットに対してパケットを送信する第3のパケット送信手段と、前記第3のパケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記第3のパケット送信手段に与える認証手段と、パケットのデータ部分を暗号化した暗号化パケットを前記第3のパケット送信手段に与える暗号化手段と、前記第3のパケット受信手段で受信したパケットの少なくともデータ部分を解読する第2の暗号解読手段と、前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末機器への転送を求めるパケットを前記第3のパケット受信手段を介して受け取り、アドレス及びプロトコルの変換を行ったものを変換パケットとして前記ゲートウェイ装置宛のパケットとして出力する際に、データ部分の暗号化されたパケットを受信した場合には暗号化パケットを前記第2の暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットをそのまま変換パケットに変換する共に、前記第2の暗号解読手段から出力されたパケットを変換パケットに変換する第2のパケット変換手段と、を具備するものであり、前記インターネット端末は、前記インターネットからパケット受信する第4のパケット受信手段と、前記インターネットに対してパケットを送信する第4のパケット送信手段と、前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、前記接続サーバ装置から前記第4のパケット受信手段を介して認証結果を受け取り、前記接続サーバに対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記第4のパケット送信手段に与えるパケット生成手段と、を具備することを特徴とするものである。

【0039】

【発明の実施の形態】(実施の形態1) 本発明の実施の形態1におけるゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステムについて、図1～図4を用いて説明する。図1は本実施の形態において、インターネット、プライベート・ネットワーク、ゲートウェイ装置、接続サーバ装置、インターネット端末、Webサーバ、プライベート端末等の接続形態を示す説明図である。

【0040】プライベート・ネットワーク1600にはプライベート端末装置として例えばPC1400、VRT1500が接続されている。このプライベート・ネット

ワーク1600はゲートウェイ装置1100を介してインターネット1700に接続されている。インターネット1700には接続サーバ装置1200、インターネット端末1300、Webサーバ1800などが接続されている。

【0041】プライベート・ネットワーク1600は家庭内の機器同士を接続しているネットワークである。ゲートウェイ装置1100は、プライベート・ネットワーク1600とインターネット1700の両方に接続され、パケットの相互変換を行うものである。

【0042】ゲートウェイ装置1100は図2に示すように、第1のパケット送信手段1101、第1のパケット受信手段1102、暗号解読手段1103、第1のパケット変換手段1104、第2のパケット受信手段1105、第2のパケット送信手段1106を含んで構成される。

【0043】第1のパケット受信手段1102はプライベート・ネットワーク1600からパケットを受信するものである。第1のパケット送信手段1101はプライベート・ネットワーク1600に対してパケットを送信するものである。第2のパケット受信手段1105はインターネット1700からパケットを受信するものである。第2のパケット送信手段1106はインターネット1700に対してパケットを送信するものである。暗号解読手段1103は、第2のパケット受信手段1105で受信した暗号化パケットの少なくともデータ部分を解読すると共に、インターネット1700に接続され、予め決められた接続サーバ装置1200のIPアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力するものである。

【0044】パケット変換手段1104は、第1のパケット受信手段1102で受信したパケットに含まれるプライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを第2のパケット送信手段1106に与えると共に、第2のパケット受信手段1105又は暗号解読手段1103から入力されたパケットのアドレス及びプロトコルの変換を行って第1のパケット送信手段1101に与えるものである。またパケット変換手段1104は、第2のパケット受信手段1105を介して接続サーバ装置1200の問い合わせパケットを受け取った場合、接続サーバ装置1200のIPアドレスを含む応答パケットを第2のパケット送信手段1106に出力する。

【0045】また接続サーバ装置1200は図3に示すように、第3のパケット送信手段1201、第3のパケット受信手段1202、暗号化手段1203、認証手段1204、第2のパケット変換手段1205を含んで構成される。

【0046】パケット受信手段1202はインターネット1700からパケットを受信するものである。パッケ

ト送信手段1201はインターネット1700に対してパケットを送信するものである。認証手段1204はパケット受信手段1202を介してインターネット1700に接続されたインターネット端末1300から認証の要求を受け取って、インターネット端末1300の認証を行い、認証結果を認証IDとして出力し、パケット送信手段1201に与えるものである。暗号化手段1203はパケットのデータ部分を暗号化してパケット送信手段1201に与えるものである。

【0047】パケット変換手段1205は、認証手段1204によって認証されたインターネット端末1300から、プライベート・ネットワーク1600に接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行った変換パケットをゲートウェイ装置1100宛のパケットとして暗号化手段1203に与えるものである。またパケット変換手段1205は、認証手段1204が送出する認証ID、及びパケット受信手段1202から受け取るパケットに含まれる認証IDを比較することによって、インターネット端末1300が認証されているか否かを判断し、認証結果が一致する場合にパケット変換するものとする。

【0048】インターネット端末1300は、インターネット1700を介してプライベート端末装置との間でパケットの通信を行うもので、図4に示すように第4のパケット送信手段1301、第4のパケット受信手段1302、パケット生成手段1303、認証要求手段1304を含んで構成される。

【0049】パケット受信手段1302はインターネット1700からパケットを受信するものである。パケット送信手段1301はインターネット1700に対してパケットを送信するものである。認証要求手段1304は、プライベート・ネットワーク1600に接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置1200に対して問い合わせを行い、接続サーバ装置1200に対して自己の端末の認証要求を行うものである。パケット生成手段1303は接続サーバ装置1200からパケット受信手段1302を介して認証結果を受け取り、接続サーバ装置1200に対してプライベート・ネットワーク1600への転送を要求するパケットを生成してパケット送信手段1301に与えるものである。

【0050】まず、プライベート・ネットワーク1600に接続されたプライベート端末装置であるPC1400が、インターネット1700に接続されたWebサーバ1800との間で通信を行う場合について以下に説明する。例えばここで行う通信とは、ホームページの閲覧などに伴う通信である。

【0051】PC1400はWebサーバ1800に対して送るべきパケットを、プライベート・ネットワーク

1600を介して先ずゲートウェイ装置1100に送信する。ゲートウェイ装置1100の第1のパケット受信手段1102はこのパケットを受信し、パケット変換手段1104に出力する。パケット変換手段1104はこのパケットのIPアドレスを付け替えた変換パケットを第2のパケット送信手段1106に出力する。第2のパケット送信手段1106はパケット変換手段1104から受け取ったパケットをインターネット1700を介してWebサーバ1800に送信する。

【0052】一方、第2のパケット受信手段1105が、上記のようにしてWebサーバ1800に送ったパケットに対する応答を含む応答パケットを受け取った場合、このパケットをパケット変換手段1104に与える。パケット変換手段1104は、このパケットのIPアドレスを付け替えてPC1400に送信するために、第1のパケット送信手段1101に出力する。第1のパケット送信手段1101から送信されたこの応答を含むパケットは、プライベート・ネットワーク1600を介してPC1400に到達する。以上のような動作によって、PC1400がインターネット1700に接続されたWebサーバ1800との間で通信を行うことができる。

【0053】ここでパケット変換手段1104が行うIPアドレスの付け替えや、応答を含むパケットの転送機能は、プロキシー（代理）サーバ機能と呼ばれている（IETFRFC 2616 Hypertext Transfer Protocol 1.1 参照）。ゲートウェイ装置1100がこのような代理サーバ機能を持っている場合、PC1400はインターネット1700に接続されたWebサーバ1800に対して送信するパケットを、ゲートウェイ装置1100に送信すればよい。ゲートウェイ装置1100は、プライベート端末装置から受け取ったパケットの発信元IPアドレスを、ゲートウェイ装置1100のインターネット1700におけるアドレスに付け替えて、すなわちゲートウェイ装置1100自身が発信するパケットとして、目的のWebサーバ1800に送信する。そして、このようにして送信したパケットに対する応答含むパケットをゲートウェイ装置1100が受け取ると、再びIPアドレスの付け替えを行って、この応答を含むパケットをプライベート・ネットワーク1600を介してプライベート端末装置に送信する。

【0054】ゲートウェイ装置1100がこのような代理サーバ機能を持つことによって、プライベート・ネットワーク1600に接続されたプライベート端末装置はインターネット1700に接続されたWebサーバ1800との間で通信を行うことができ、結果としてホームページの閲覧ができる。

【0055】なお、送信したパケットに対する応答を含むパケットの識別は、TCP/IPの通信で用いられるポート番号によって行うことができる。ゲートウェイ装

置1100がWebサーバ1800に送信したパケットには、パケット変換手段1104によって指定されたポート番号が含まれおり、この送信パケットに対応した応答を含むパケットにも、ここで指定したポート番号が含まれている。このため、パケット変換手段1104は、Webサーバ1800のIPアドレスとポート番号を確認することで、送信済みのどのパケットに対する応答であるかを識別することができる。

【0056】次に、インターネット1700に接続されたインターネット端末1300が、プライベート・ネットワーク1600に接続されたVTR1500との間で通信を行う場合について以下に説明する。このような通信とは、インターネット1700に接続されたインターネット端末1300から、VTR1500の動作制御や状態問い合わせ等を行う場合である。

【0057】インターネット端末1300の認証要求手段1304は、VTR1500への通信に先だって、まずゲートウェイ装置1100に対して接続サーバ装置の問い合わせ要求を行う。インターネット端末1300の認証要求手段1304は、この問い合わせ要求を含むパケットをパケット送信手段1301に与える。パケット送信手段1301はこのパケットをインターネット1700を介して、ゲートウェイ装置1100の第2のパケット受信手段1105に送信する。第2のパケット受信手段1105がこの問い合わせを含むパケットを受信すると、パケット変換手段1104に与える。パケット変換手段1104はこの問い合わせに対する応答として、接続サーバ装置1200のIPアドレスを含むパケットを第2のパケット送信手段1106に与える。第2のパケット送信手段1106はこの応答を含むパケットをインターネット端末1300に送信する。インターネット端末1300のパケット受信手段1302は、このパケットを受信して認証要求手段1304に出力する。

【0058】次に認証要求手段1304は、上記の問い合わせによってIPアドレスを受け取った接続サーバ装置1200に対して、認証要求を含むパケットを出力する。インターネット端末1300のパケット送信手段1301によって送信された認証要求を含むパケットは、インターネット1700を介して接続サーバ装置1200のパケット受信手段1202によって受信される。接続サーバ装置1200のパケット受信手段1202は、この認証要求を含むパケットを認証手段1204に与える。認証手段1204がこのパケットを受け取ると、予め定められた方法によって認証要求を検査し、VTR1500との間での通信を許可できるか否かを判断する。なおここで行う認証の判断は、例えばインターネット端末1300が予め登録されたものであるか否か、またパスワードや暗証番号の確認等によって行うことができる。また、認証の方法によっては複数のパケットの送受信を伴う場合もある。

【0059】この判断の結果、認証手段1204はインターネット端末1300に対してVTR1500との間の通信を許可する場合には、認証の結果として認証IDを含むパケットを出力し、通信を許可しない場合には認証の失敗を示すパケットを出力し、パケット送信手段1201に与える。パケット送信手段1201は、このパケットをインターネット1700に送信する。インターネット端末1300のパケット受信手段1302がこのパケット受信すると、認証要求手段1304に与える。

【0060】上記のような認証手続きの結果、インターネット端末1300がVTR1500との間の通信を許可された場合、パケット生成手段1303はVTR1500に送信するパケットに加えて、認証要求手段1304から受け取る認証IDおよび接続サーバ装置1200のIPアドレスを使用して、VTR1500に対しての転送を要求するパケットを生成してパケット送信手段1301に出力する。パケット送信手段1301はこのパケットをインターネット1700を介して接続サーバ装置1200に送信する。

【0061】接続サーバ装置1200のパケット受信手段1202は、インターネット端末1300によって送信されたVTR1500への転送を要求するパケットを受信し、これをパケット変換手段1205に与える。パケット変換手段1205は、パケット受信手段1202から受け取ったパケットに含まれる認証IDと、インターネット端末1300のIPアドレスとを認証手段1204から受け取ると、通信を許可した端末の認証IDとIPアドレスとの組み合わせと比較し、このパケットが認証手段1204によって通信が許可されたものであるか否かを確認する。そして許可されているパケットの場合には、受け取ったパケットをデータ部分に含むパケットを新たに生成し、暗号化手段1203に与える。このようなパケットのデータ部分に別のパケットを含めて通信する方法は、パケットのカプセル化と呼ばれている。

【0062】暗号化手段1203は、受け取ったパケットのデータ部分を、予めゲートウェイ装置1100との間で決められた方法によって暗号化した暗号化パケットをパケット送信手段1201に与える。パケット送信手段1201はこの暗号化パケットをインターネット1700を介してゲートウェイ装置1100に送信する。

【0063】ゲートウェイ装置1100の第2のパケット受信手段1105が暗号化パケットを受信すると、このパケットを暗号解読手段1103に与える。暗号解読手段1103は、接続サーバ装置1200から送信されたパケットのみを受け取り、接続サーバ装置1200との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段1104に出力される。一方、暗号の解読が正常に行われなかったパケット、及び接続サーバ装置1200以外から受け取ったパケットは破棄される。

【0064】パケット変換手段1104は前述の代理サーバに相当する機能を持ち、暗号解読手段1103から受け取ったパケットのデータ部分から、カプセル化されたパケットを取り出し、IPアドレスの付け替え等を行って第1のパケット送信手段1101に与える。第1のパケット送信手段1101は、このパケットをゲートウェイ装置1100が発信するパケットとして、プライベート・ネットワーク1600を介してVTR1500に送信する。

【0065】VTR1500は、ゲートウェイ装置1100によって送信されたパケットを受信すると、この受信パケットに対する応答を含むパケットをゲートウェイ装置1100に送信する。ゲートウェイ装置1100の第1のパケット受信手段1102は受信したパケットをパケット変換手段1104に与える。パケット変換手段1104はIPアドレスの付け替え等を行った変換パケットを第2のパケット送信手段1106に与える。第2のパケット送信手段1106はこのパケットをインターネット1700を介してインターネット端末1300に送信する。

【0066】このようにして、インターネット1700に接続されたインターネット端末1300と、プライベート・ネットワークに接続されたVTR1500との間での通信が可能となる。即ちインターネット端末1300がVTR1500の動作制御等を行うことができる。これにより、例えば家の外から、家庭内にあるVTRの録画予約、予約状況の確認等を行うことができる。

【0067】以上のように接続サーバ装置1200がインターネット端末1300の認証を行い、またゲートウェイ装置1100は接続サーバ装置1200から送信されたパケットのみを受信することで、接続サーバ装置1200において高いセキュリティを実現し、ゲートウェイ装置1100の処理負荷を軽減することができる。こうしてインターネット1700からプライベート・ネットワーク1600へのアクセスが可能となる。ここで、セキュリティの強さは接続サーバ装置1200の認証手段1204によって決まるものであり、必要に応じて新しく又は強固なものに更新することができる。このため、ゲートウェイ装置1100の置き換えや、機能の更新等を行うことなく、ゲートウェイ装置1100及びプライベート・ネットワーク1600のセキュリティの強化が実現される。

【0068】更に接続サーバ装置1200は、ゲートウェイ装置1100と同等の機能を有する他の複数のゲートウェイ装置に対して同様の機能を発揮することができる。このような場合、接続サーバ装置1200のセキュリティを強化することで、多数のゲートウェイ装置及びプライベート・ネットワークのセキュリティを強化することができるとなり、個々のゲートウェイ装置のセキュリティを強化する場合に比べて、効率的かつ迅速な対応が

可能となる。

【0069】なお、インターネット端末1300が、予め接続サーバ装置1200のIPアドレスを知りていれば、ゲートウェイ装置1100に対して接続先の問い合わせを行わずに、接続サーバ装置1200に対して直接認証要求を行うことができる。またこのような場合、ゲートウェイ装置1100のインターネット1700側のIPアドレスが動的な割り当てにより変化する場合でも、上記と同等の機能を実現することが可能となる。更には、ゲートウェイ装置1100のIPアドレスがインターネット1700に接続された他の機器に知られることがないため、より高いセキュリティの実現できる。

【0070】上記のような夫々の装置の動作に加えて、ゲートウェイ装置1100のパケット変換手段1104がWebサーバ機能を有する場合、インターネット端末1300によって送信されたパケットをVTR1500に転送するのではなく、このWebサーバがパケットを処理し、その結果生成されたパケットをVTR1500に送信することもできる。このような場合、インターネット端末1300は、パケット変換手段1104のWebサーバにアクセスしてVTR1500に要求する動作に対応する入力や選択等を行う。このWebサーバは入力パケットを処理し、VTR1500への動作制御を行うためのパケットを生成し、第1のパケット送信手段1101を介してVTR1500に送信する。またVTR1500から送信された応答は、パケット変換手段1104のWebサーバによって受け取られる。WebサーバはWebページの更新を行うことによって、VTR1500から受け取った応答をインターネット端末1300に提示することができる。

【0071】なお、プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するシステムを、ネットワークシステムと呼ぶ。

【0072】このようにゲートウェイ装置1100のパケット変換手段1104がWebサーバ機能を持つことによって、インターネット端末1300はVTR1500の動作制御を直接行う必要がなくなる。この場合、インターネット端末1300には、VTR1500を制御するための専用のソフトウェアを用意しなくても、汎用のブラウザ等によってVTR1500の動作を制御することができる。

【0073】(実施の形態2) 次に本発明の実施の形態2におけるゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステムについて、図5～図8を用いて説明する。図5は本実施の形態において、インターネット、プライベート・ネットワーク、ゲートウェイ装置、接続サーバ装置、インターネット端末、Webサーバ、プライベート端末等の接続形態を示す説明

図である。

【0074】プライベート・ネットワーク2600にはプライベート端末装置として、例えばPC2400、VTR2500が接続されている。このプライベート・ネットワーク2600はゲートウェイ装置2100を介してインターネット2700に接続されている。インターネット2700には接続サーバ装置2200、インターネット端末2300、Webサーバ2800などが接続されている。

【0075】プライベート・ネットワーク2600は家庭内の機器同士を接続しているネットワークである。ゲートウェイ装置2100は、プライベート・ネットワーク2600とインターネット2700の両方に接続され、パケットの相互変換を行うものである。

【0076】ゲートウェイ装置2100は図6に示すように、第1のパケット送信手段2101、第1のパケット受信手段2102、第1の暗号解読手段2103、第1のパケット変換手段2104、第1の暗号化手段2105、第2のパケット受信手段2106、第2のパケット送信手段2107を含んで構成される。

【0077】第1のパケット受信手段2102はプライベート・ネットワーク2600からパケットを受信するものである。第1のパケット送信手段2101はプライベート・ネットワーク2600に対してパケットを送信するものである。第2のパケット受信手段2106はインターネット2700からパケットを受信するものである。第2のパケット送信手段2107はインターネット2700に対してパケットを送信するものである。

【0078】暗号化手段2105はパケットのデータ部分を暗号化し、暗号化パケットを第2のパケット送信手段2107に与えるものである。暗号解読手段2103は第2のパケット受信手段2106で受信したパケットの少なくともデータ部分を解読するものである。尚、暗号解読手段2103は、インターネット2700に接続され、予め決められた接続サーバ装置2200のIPアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力するものとする。

【0079】パケット変換手段2104は、第1のパケット受信手段2102で受信したパケットに含まれるプライベート端末装置のアドレス及びプロトコルの変換を行ったパケットを暗号化手段2105に出力すると共に、暗号解読手段2103から受け取ったパケットのアドレス及びプロトコルの変換を行って第1のパケット送信手段2101に与えるものである。またパケット変換手段2104は、第1のパケット受信手段2102から受け取ったパケットを、インターネット2700に接続されて予め決められた接続サーバ装置2200宛のパケットとして、暗号化手段2105に与える。更にパケット変換手段2104は、第2のパケット受信手段2106を介して接続サーバ装置2200の問い合わせパッ

トを受け取った場合、接続サーバ装置2200のIPアドレスを含む応答パケットを第2のパケット送信手段2107に与えるものとする。

【0080】次に接続サーバ装置2200は図7に示すように、第3のパケット送信手段2201、第3のパケット受信手段2202、第2の暗号化手段2203、認証手段2204、第2の暗号解読手段2205、第2のパケット変換手段2206を含んで構成される。

【0081】パケット受信手段2202はインターネット2700からパケットを受信するものである。パケット送信手段2201はインターネット2700に対してパケットを送信するものである。認証手段2204は、パケット受信手段2202を介して、インターネット2700に接続されたインターネット端末2300から認証の要求を受け取って、インターネット端末2300の認証を行い、認証結果をパケット送信手段2201に与えるものである。

【0082】暗号化手段2203はパケットのデータ部分を暗号化してパケット送信手段2201に与えるものである。暗号解読手段2205はパケット受信手段2202で受信したパケットの少なくともデータ部分を解読するものである。尚、暗号解読手段2205は、ゲートウェイ装置2100のIPアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力するものとする。

【0083】パケット変換手段2206は、認証手段2204によって認証されたインターネット端末2300から、プライベート・ネットワーク2600に接続されたプライベート端末機器への転送を求めるパケットを、パケット受信手段2202を介して受け取り、アドレス及びプロトコルの変換を行った変換パケットをゲートウェイ装置2100宛のパケットとして暗号化手段2203に与えるものである。尚、パケット変換手段2206は、代理サーバ機能を持ち、暗号解読手段2205から受け取ったパケットのデータ部分に含まれるパケットの発信元IPアドレスとして、接続サーバ装置2200のIPアドレスを付加して出力するものとする。そしてパケット変換手段2206は認証手段2204が出力する認証ID、及びパケット受信手段2202から受け取るパケットに含まれる認証IDを比較することによって、インターネット端末2300が認証されているか否かを判断し、認証結果が一致する場合にパケット変換する。

【0084】尚、パケット受信手段2202は、データ部分の暗号化されたパケットを受信した場合には暗号化パケットを暗号解読手段2205に与え、暗号化されていないパケットを受信した場合に非暗号化パケットをパケット変換手段2206に与えるものとする。

【0085】インターネット端末2300は、インターネット2700を介してプライベート端末装置であるPC2400やVTR2500との間でパケットの通信を

行うもので、図8に示すように第4のパケット送信手段2301、第4のパケット受信手段2302、パケット生成手段2303、認証要求手段2304を含んで構成される。これらの構成要素と各構成要素の機能は、実施の形態1と同様であるので、説明を省略する。

【0086】まず、プライベート端末装置であるPC2400が、インターネット2700に接続されたWebサーバ2800との間で通信を行う場合について以下に説明する。ここで行う通信とは、例えばホームページの閲覧などに伴う通信である。

【0087】PC2400は、Webサーバ2800に対して送るべきパケットを、先ずプライベート・ネットワーク2600を介してゲートウェイ装置2100に送信する。ゲートウェイ装置2100の第1のパケット受信手段2102はこのパケットを受信すると、パケット変換手段2104に与える。パケット変換手段2104は受け取ったパケットをデータ部分に含むパケットを生成し、変換パケットに変換して暗号化手段2105に与える。このように、パケットのデータ部分に別のパケットを含めて通信する方法は、パケットのカプセル化と呼ばれている。

【0088】暗号化手段2105は受け取ったパケットのデータ部分を、接続サーバ装置2200との間で予め定められた方法で暗号化して暗号化パケットを生成し、第2のパケット送信手段2107に与える。第2のパケット送信手段2107は、暗号化手段2105から受け取った暗号化パケットをインターネット2700を介して接続サーバ装置2200に送信する。

【0089】接続サーバ装置2200のパケット受信手段2202は、暗号化パケットを受信して暗号解読手段2205に与える。暗号解読手段2205はゲートウェイ装置2100から送信されたパケットのみを受け取り、ゲートウェイ装置2100との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段2206に出力され、暗号の解読が正常に行われなかったパケット、及びゲートウェイ装置2100以外から受け取ったパケットは破棄される。

【0090】パケット変換手段2206は、暗号の解読されたパケットのデータ部分から、ゲートウェイ装置2100がPC2400から受信した形式のパケットを取り出す。またパケット変換手段2206は、実施の形態1におけるゲートウェイ装置2100のパケット変換手段2104と同様に代理サーバ機能を持つ。即ち、暗号解読手段2205から受け取ったパケットのデータ部分より取り出したパケットに対して、IPアドレスの付け替えを行い、パケット送信手段2201に与える。パケット送信手段2201は、受け取ったパケットをインターネット2700を介してWebサーバ2800に送信する。

【0091】一方、接続サーバ装置2200のパケット受信手段2202が、上記のようにしてWebサーバ2800に送ったパケットに対する応答を含む応答パケットを受け取ると、パケット受信手段2202はこの応答パケットをパケット変換手段2206に与える。パケット変換手段2206は代理サーバの機能によるIPアドレスを付け替え等を行い、このパケットをデータ部分に含むパケットを生成して暗号化手段2203に与える。暗号化手段2203は、受け取ったパケットのデータ部分を、ゲートウェイ装置2100との間で予め定められた方法で暗号化し、暗号化パケットをパケット送信手段2201に与える。パケット送信手段2201はこの暗号化パケットをインターネット2700を介してゲートウェイ装置2100に送信する。

【0092】ゲートウェイ装置2100の第2のパケット受信手段2106は、上記の暗号化パケットを受信して暗号解読手段2103に与える。暗号解読手段2103は接続サーバ装置2200から送信されたパケットのみを受け取り、接続サーバ装置2200との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段2104に出力され、暗号の解読が正常に行われなかったパケット、及び接続サーバ装置2200以外から受け取ったパケットは破棄される。

【0093】パケット変換手段2104は、暗号解読手段2103から受け取ったパケットのデータ部分に含まれるパケットを取り出して、第1のパケット送信手段2101に与える。第1のパケット送信手段2101はこのパケットをプライベート・ネットワーク1600を介してPC2400に送信する。

【0094】以上のような動作によって、PC2400がインターネット2700に接続されたWebサーバ2800との間で通信を行うことができ、結果としてWebサーバ2800に備えられたホームページの閲覧などが行える。

【0095】次に、インターネット2700に接続されたインターネット端末2300が、プライベート・ネットワーク2600に接続されたVTR2500との間で通信を行う場合について以下に説明する。このような通信とは、例えばインターネット2700に接続されたインターネット端末装置2300から、VTR2500の動作制御や状態問い合わせ等を行うものである。

【0096】インターネット端末2300の認証要求手段2304は、VTR2500への通信に先だって、まずゲートウェイ装置2100に対して接続サーバ装置の問い合わせ要求を行う。この問い合わせ要求を含むパケットは、インターネット端末2300のパケット送信手段2301によって、インターネット2700を介してゲートウェイ装置2100の第2のパケット受信手段2106に送信される。第2のパケット受信手段2106

がこの問い合わせを含むパケットを受信すると、このパケットをパケット変換手段2104に与える。パケット変換手段2104はこの問い合わせに対する応答として、接続サーバ装置2200のIPアドレスを含む応答パケットを第2のパケット送信手段2107に与える。第2のパケット送信手段2107はこの応答パケットをインターネット端末2300に送信する。インターネット端末2300のパケット受信手段2302はこのパケットを受信して認証要求手段2304に与える。

【0097】次に認証要求手段2304は、上記の問い合わせによってIPアドレスを受け取った接続サーバ装置2200に対して、認証要求を含むパケットを出力する。認証要求を含むパケットがインターネット2700を介して接続サーバ装置2200のパケット受信手段2202によって受信されると、パケット受信手段2202は、この認証要求を含むパケットを認証手段2204に与える。認証手段2204はこのパケットを受け取ると、この認証要求を予め定められた方法によって検査し、VTR2500との間での通信を許可できるか否かを判断する。尚、ここで行う認証の判断は、例えばインターネット端末2300が予め登録されたものであるか否か、又はパスワードや暗証番号の確認等によって行うことができる。また、認証の方法によっては、複数のパケットの送受信を伴う場合もある。

【0098】この判断の結果、認証手段2204はインターネット端末2300にVTR2500との間の通信を許可する場合には、認証の結果として認証IDを含むパケットをパケット送信手段2201に与え、通信を許可しない場合には認証の失敗を示すパケットをパケット送信手段2201に与える。パケット送信手段2201はこのパケットをインターネット2700に送信する。インターネット端末2300のパケット受信手段2302がこのパケットを受信すると、認証要求手段2304に与える。

【0099】上記のような認証手続きの結果、インターネット端末2300がVTR2500との間の通信を許可された場合、パケット生成手段2303はVTR2500に送信するパケットに加えて、認証要求手段2304から受け取る認証IDおよび接続サーバ装置2200のIPアドレスを使用して、VTR2500に対しての転送を要求するパケットを生成し、パケット送信手段2301に与える。パケット送信手段2301はこのパケットをインターネット2700を介して接続サーバ装置2200に送信する。

【0100】接続サーバ装置2200のパケット受信手段2202は、インターネット端末2300から送信されたVTR2500への転送を要求するパケットを受信すると、このパケットをパケット変換手段2206に与える。

【0101】パケット変換手段2206は、パケット受

信手段2202から受け取ったパケットに含まれる認証IDとインターネット端末2300のIPアドレスを、認証手段2204から受け取り、通信を許可した端末の認証ID及びIPアドレスとの組み合わせを比較する。そして、このパケットが認証手段2204によって通信が許可されたものであるか否かを確認する。この確認によって許可されているパケットの場合には、代理サーバの機能によるIPアドレスを付け替え等を行い、このパケットをデータ部分に含む変換パケットを生成し、暗号化手段2203に与える。

【0102】暗号化手段2203は、受け取ったパケットのデータ部分を、ゲートウェイ装置2100との間で予め定められた方法で暗号化し、暗号化パケットをパケット送信手段2201に与える。パケット送信手段2201はこの暗号化パケットをインターネット2700を介してゲートウェイ装置2100に送信する。

【0103】ゲートウェイ装置2100の第2のパケット受信手段2106がこの暗号化されたパケットを受信すると、このパケットを暗号解読手段2103に与える。暗号解読手段2103は接続サーバ装置2200から送信されたパケットのみを受け取り、接続サーバ装置2200との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段2104に出力され、暗号の解読が正常に行われなかったパケット、及び接続サーバ装置2200以外から受け取ったパケットは破棄される。

【0104】パケット変換手段2104は、暗号解読手段2103から受け取ったパケットのデータ部分に含まれるパケットを取り出して、第1のパケット送信手段2101に出力する。第1のパケット送信手段2101はこのパケットをプライベート・ネットワーク2600を介して、VTR2500に送信する。

【0105】VTR2500はゲートウェイ装置2100によって送信されたパケットを受信すると、このパケットに対する応答を含む応答パケットをゲートウェイ装置2100に送信する。ゲートウェイ装置2100の第1のパケット受信手段2102は、受信した応答パケットをパケット変換手段2104に与える。パケット変換手段2104は、受け取ったパケットをデータ部分に含む変換パケットを生成し、暗号化手段2105に与える。

【0106】暗号化手段2105は、受け取ったパケットのデータ部分を、接続サーバ装置2200との間で予め定められた方法で暗号化し、暗号化パケットを第2のパケット送信手段2107に与える。第2のパケット送信手段2107は、暗号化手段2105から受け取った暗号化パケットをインターネット2700を介して接続サーバ装置2200に対して送信する。

【0107】接続サーバ装置2200のパケット受信手段2202は、上記の暗号化されたパケットを受信して

暗号解読手段2205に与える。暗号解読手段2205はゲートウェイ装置2100から送信されたパケットのみを受け取り、ゲートウェイ装置2100との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段2206に出力され、暗号の解読が正常に行われなかったパケット、及びゲートウェイ装置2100以外から受け取ったパケットは破棄される。

【0108】パケット変換手段2206は、暗号の解読されたパケットのデータ部分から、ゲートウェイ装置2100を介してVTR2500から受信したパケットを取り出す。またパケット変換手段2206は、実施の形態1におけるゲートウェイ装置1100のパケット変換手段1104と同様に代理サーバ機能を持つ。従ってパケット変換手段2206は、暗号解読手段2205から受け取ったパケットのデータ部分より取り出したパケットに対して、IPアドレスの付け替えを行ってパケット送信手段2201に与える。パケット送信手段2201は受け取ったパケットを、インターネット2700を介してインターネット端末2300に送信する。

【0109】このようにして、インターネット2700に接続されたインターネット端末2300と、プライベート・ネットワーク2600に接続されたVTR2500との間で通信が可能となる。即ちインターネット端末2300がVTR2500の動作制御等を行うことができる。これにより、例えば家の外から家庭内にあるVTRの録画予約や予約状況の確認等を行うことができる。

【0110】以上に示したゲートウェイ装置2100と接続サーバ装置2200は、従来使用されているファイア・ウォールの機能を発揮しているものと考えることができる。即ち、ファイア・ウォールにおけるプライベート・ネットワーク2600側の機能をゲートウェイ装置2100で実現し、インターネット2700側の機能を接続サーバ装置2200で実現している。これは両者の間をインターネットを使用した仮想プライベート・ネットワークで接続したものと考えることができる。

【0111】またゲートウェイ装置2100と接続サーバ装置2200の間を暗号化されたパケットで通信を行い、更にゲートウェイ装置2100は接続サーバ装置2200から送信されたパケットのみを受信し、プライベート・ネットワーク2600に転送することにより、接続サーバ装置2200において高いセキュリティを確保している。そしてゲートウェイ装置2100の処理負荷を軽減し、且つインターネット2700とプライベート・ネットワーク2600との相互通信を可能にしている。

【0112】ここで、セキュリティの強さは接続サーバ装置2200の認証手段2204によって決まるので、必要に応じて新しく、又は強固なものに更新することができる。このため、ゲートウェイ装置2100の置き換

えや機能の更新等を行うことなく、ゲートウェイ装置及びプライベート・ネットワークのセキュリティの強化が確保される。

【0113】更に接続サーバ装置2200は、ゲートウェイ装置2100と同等の機能を有する他の複数のゲートウェイ装置に対して、同様の機能を発揮することができる。このような場合、接続サーバ装置2200のセキュリティを強化することで、多数のゲートウェイ装置及びプライベート・ネットワークのセキュリティを強化することができる。このことは夫々のゲートウェイ装置のセキュリティを強化する場合に比べて、効率的かつ迅速な対応ができるることを意味する。

【0114】なお、インターネット端末2300が、予め接続サーバ装置2200のIPアドレスを知りていれば、接続先の問い合わせを行わずに、接続サーバ装置2200に対して直接認証要求を行うことができる。またこのような場合、ゲートウェイ装置2100のインターネット2700側のIPアドレスが動的な割り当てにより変化する場合でも、上記と同等の機能を確保することができる。更には、ゲートウェイ装置2100のIPアドレスが、インターネットに接続された機器に知られることがないため、より高いセキュリティが確保される。

【0115】上記のような夫々装置の動作に加えて、接続サーバ装置2200のパケット変換手段2206がWebサーバの機能を持つ場合、インターネット端末2300によって送信されたパケットをゲートウェイ装置2100に転送するのではなく、このWebサーバによって処理されて生成されたパケットを、ゲートウェイ装置2100に直接送信することもできる。このような場合、認証手段2204によってプライベート・ネットワーク2600へのアクセスを許可されたインターネット端末2300は、パケット変換手段2206のWebサーバにアクセスして、VTR2500に要求する動作に対応する入力や選択等を行うことができる。

【0116】この場合、Webサーバ2800は入力を処理し、VTR2500への動作制御を行うためのパケットを生成し、暗号化手段2203に出力する。パケット変換手段2206によって生成されたパケットは、上記と同様に暗号化されてゲートウェイ装置2100に送信され、ゲートウェイ装置2100で暗号を解読されてVTR2500に送信される。またVTR2500から送信された応答は、パケット変換手段2206のWebサーバによって受け取られる。この応答を受けたWebサーバはWebページの更新を行うことによって、VTR2500から受け取った応答をインターネット端末2300に提示することができる。

【0117】このように接続サーバ装置2200のパケット変換手段2206がWebサーバ機能を持つことによって、インターネット端末2300はVTR2500の動作制御を直接行う必要がなくなる。このため、イン

ターネット端末2300には、VTR2500を制御するための専用のソフトウェアを用意しなくとも、汎用のプラウザ等によってVTR2500の動作制御が可能となる。

【0118】

【発明の効果】以上のように本発明によれば、プライベート・ネットワークに設置するゲートウェイ装置の処理負担を小さくし、かつプライベート・ネットワークのセキュリティを確保した上で、プライベート・ネットワークとインターネットの相互接続が可能となる。

【0119】さらにはゲートウェイ装置に実装される機能の追加や更新を行わなくても、接続サーバ装置側での認証機能を更新したり追加することによって、プライベート・ネットワークのセキュリティの強化が可能になるという効果が得られる。

【図面の簡単な説明】

【図1】本発明の実施の形態1におけるゲートウェイ装置、接続サーバ装置、インターネット端末の接続関係(ネットワークシステム)を示す説明図である。

【図2】実施の形態1におけるゲートウェイ装置の構成を示すブロック図である。

【図3】実施の形態1における接続サーバ装置の構成を示すブロック図である。

【図4】実施の形態1におけるインターネット端末の構成を示すブロック図である。

【図5】本発明の実施の形態2におけるゲートウェイ装置、接続サーバ装置、インターネット端末の接続関係(ネットワークシステム)を示す説明図である。

【図6】実施の形態2におけるゲートウェイ装置の構成を示すブロック図である。

【図7】実施の形態2における接続サーバ装置の構成を示すブロック図である。

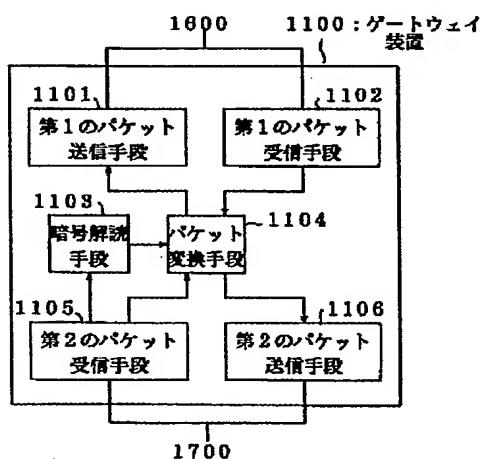
示すブロック図である。

【図8】実施の形態2におけるインターネット端末の構成を示すブロック図である。

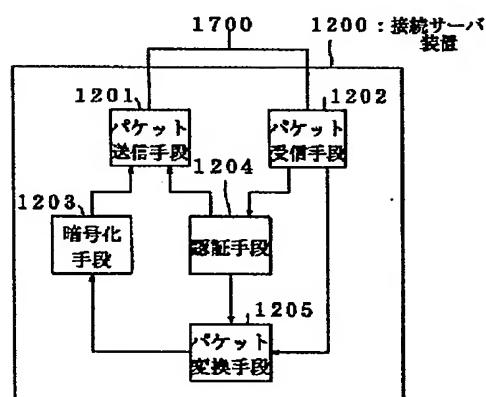
【符号の説明】

- 1100, 2100 ゲートウェイ装置
- 1101, 2101 第1のパケット送信手段
- 1102, 2101 第1のパケット受信手段
- 1103 暗号解読手段
- 1104, 2104 第1のパケット変換手段
- 1105, 2105 第2のパケット受信手段
- 1106, 2107 第2のパケット送信手段
- 1200, 2200 接続サーバ装置
- 1201, 2101 第3のパケット送信手段
- 1202, 2202 第3のパケット受信手段
- 1203 暗号化手段
- 2105 第1の暗号化手段
- 2203 第2の暗号化手段
- 1204, 2204 認証手段
- 1205, 2206 第2のパケット変換手段
- 1300, 2300 インターネット端末
- 1301, 2301 第4のパケット送信手段
- 1302, 2302 第4のパケット受信手段
- 1303, 2303 パケット生成手段
- 1304, 2304 認証要求手段
- 1400, 2400 PC
- 1500, 2500 VTR
- 1600, 2600 プライベート・ネットワーク
- 1700, 2700 インターネット
- 1800, 2800 Webサーバ
- 2103 第1の暗号解読手段
- 2205 第2の暗号解読手段

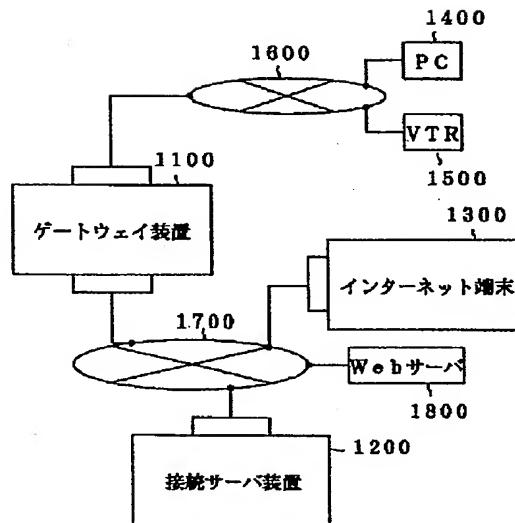
【図2】



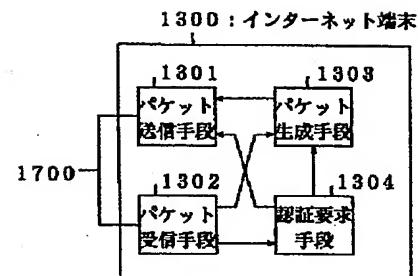
【図3】



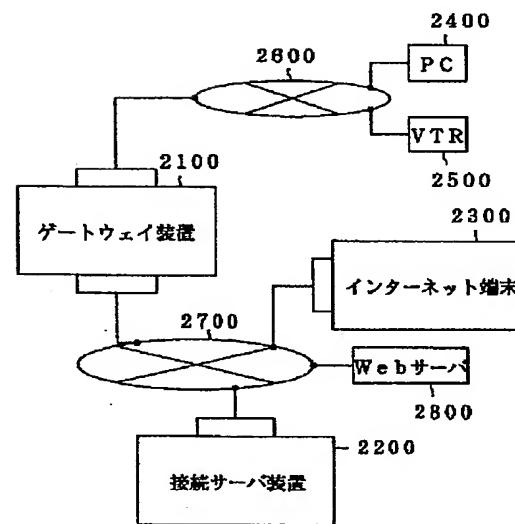
【図1】



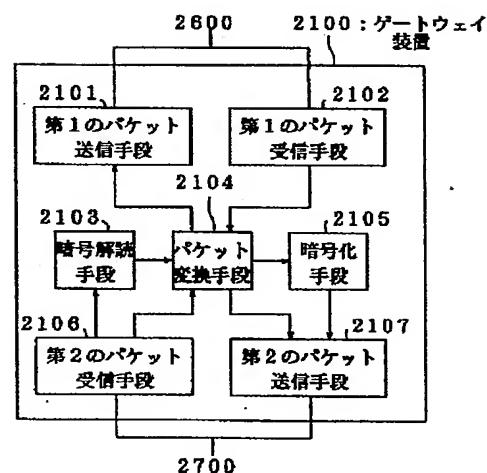
【図4】



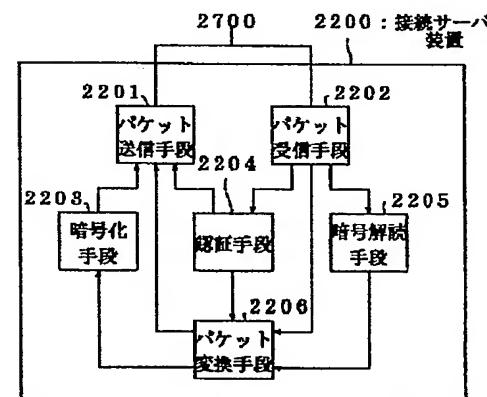
【図5】



【図6】



【図7】



(20) 01-326695 (P2001-32 [JL8]

【図8】

